SSO, MFA, Blackbaud ID & Your Org's Security Posture

blackbaud®
DEVELOPERS' CONFERENCE
June 15–17, 2021

BLACKBAUD SKY® TRACK

JOHN VOGEL

Session Host: Dave Evatt

Safe Harbor Statement

This presentation contains forward-looking statements that involve inherent risks, uncertainties and assumptions. It outlines Blackbaud's current plans and general product direction as of the date this presentation was created. Functionality described in this presentation that is not currently available is subject to change at any time, without notice, at Blackbaud's sole discretion. It does not represent a commitment to develop or release specific features within the timeframe discussed, according to the presented design, or at all. Please make any purchase decisions based on features and functionality that are currently available.

Customization of Blackbaud Solutions

As a Blackbaud customer, your Authorized Support Contacts retain the responsibility for providing internal support for Customizations of your Blackbaud solutions by:

- Providing direct support to answer questions regarding Subscription functionality, internal business practices, and troubleshooting processes to Your Non-Authorized Users
- Providing direct support to answer questions regarding Customization specifications, features, intended usage, and Error correction and troubleshooting processes to Your Non-Authorized Users

Hello! I'm John Vogel

Pronouns: He/Him/His

CHARLESTON, SC

2 YEARS AT BLACKBAUD

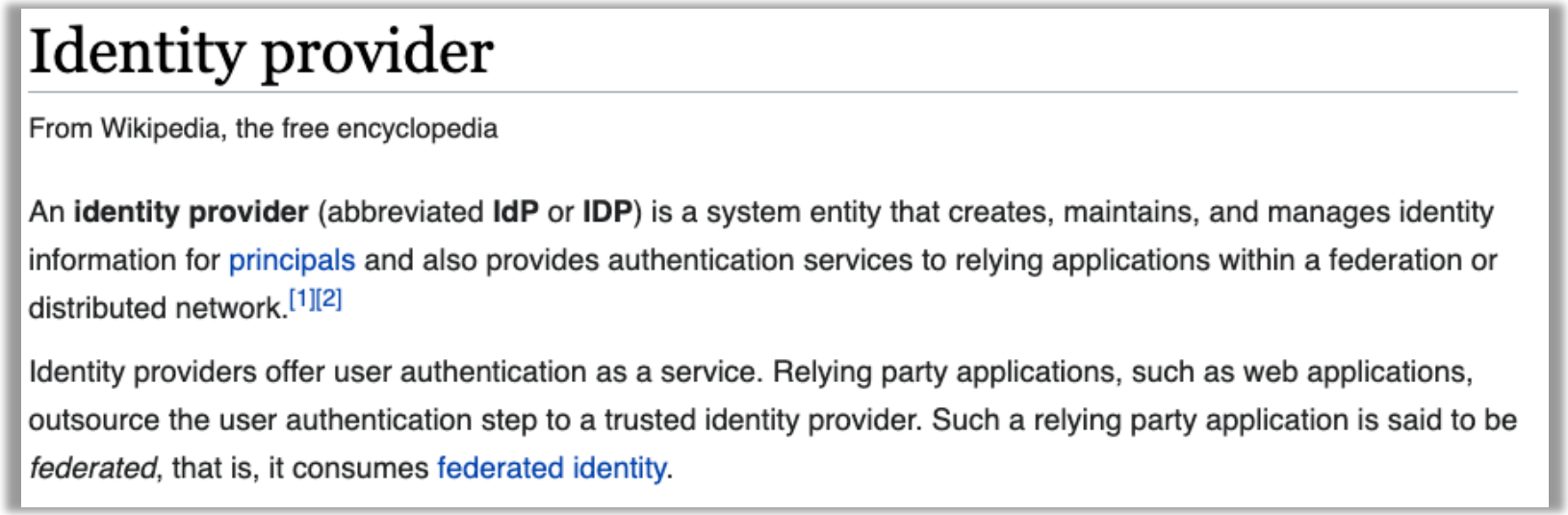
Ocean or Mountains? I choose both by living 10 minutes from the beach with family and taking winter vacations to go snowboarding.

Questions we'll answer today

- What's involved with establishing an SSO connection with Blackbaud ID?
- Who should be on SSO?
- Who should go through MFA?

Identity Provider (IdP)

Wikipedia Definition



Identity provider

From Wikipedia, the free encyclopedia

An **identity provider** (abbreviated **IdP** or **IDP**) is a system entity that creates, maintains, and manages identity information for principals and also provides authentication services to relying applications within a federation or distributed network.[1][2]

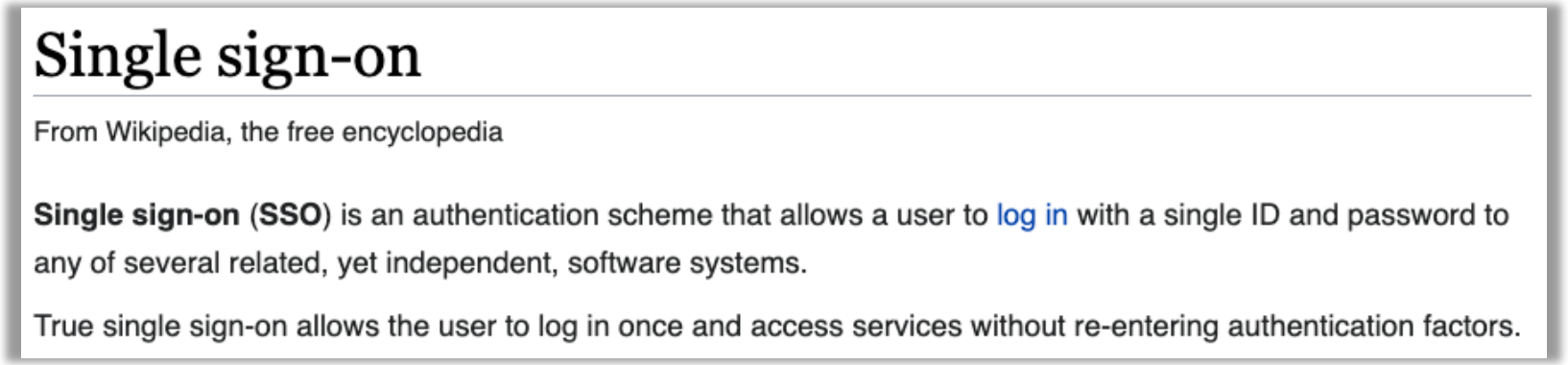
Identity providers offer user authentication as a service. Relying party applications, such as web applications, outsource the user authentication step to a trusted identity provider. Such a relying party application is said to be *federated*, that is, it consumes federated identity.

If you only remember 1 thing

IdPs prove who your users are so they can sign in to applications.

Single Sign-On (SSO)

Wikipedia Definition



Single sign-on

From Wikipedia, the free encyclopedia

Single sign-on (**SSO**) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems.

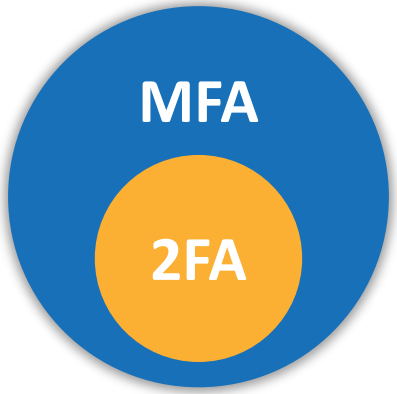
True single sign-on allows the user to log in once and access services without re-entering authentication factors.

If you only remember 1 thing

SSO allows users to quickly sign in to applications using credentials they're familiar

Multi-Factor Authentication (MFA)

Wikipedia Definition



Multi-factor authentication (**MFA**; encompassing **Two-factor authentication** or **2FA**, along with similar terms) is an electronic authentication method in which a device user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). MFA protects the user from an unknown person trying to access their data such as personal ID details or financial assets.

If you only remember 1 thing

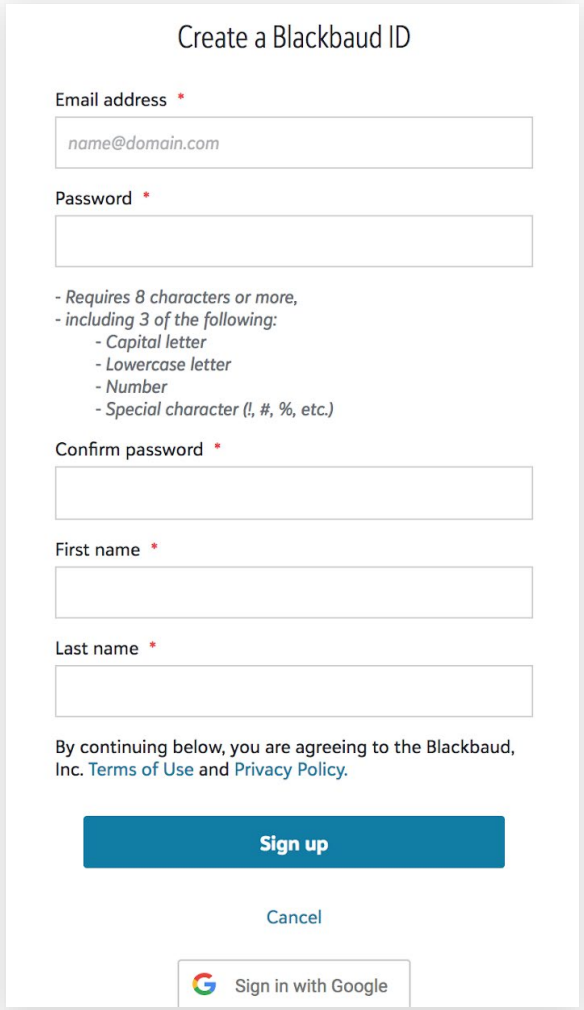
Having MFA turned on is the greatest single measure to increase the security of an account.

#bbdevdays

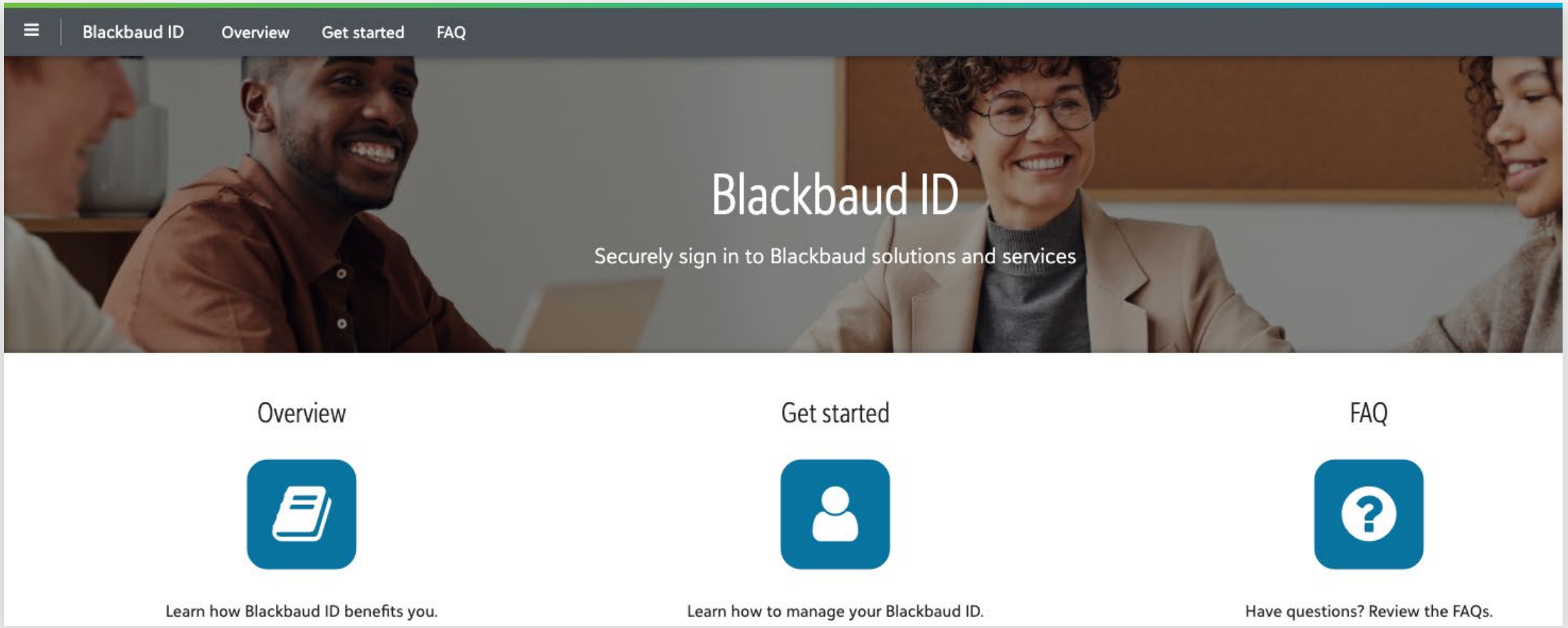
Thanks for the 101 on industry terms, but how do these play with Blackbaud ID?

What is Blackbaud ID?

- Centralized **authentication**, **identity** and **session management** providing users with a SSO for the Blackbaud solution ecosystem
- Self-serve **user registration** process to create their account
- **SSO** configuration for federated identity with your identity provider (ex: Azure, Okta, Google)
- Enables **MFA** or further options through an identity provider
- **Social Sign In**: Google Account



Blackbaud ID Resource Site



https://docs.blackbaud.com/bbid-docs/

Signing in to Blackbaud ID

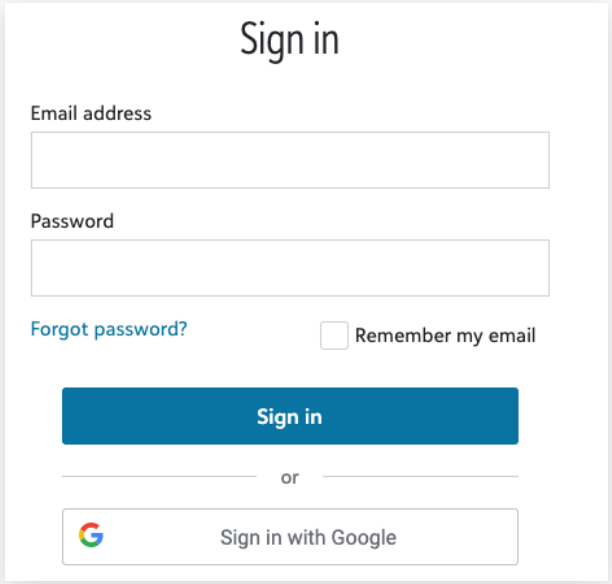
Users can sign in via 3 methods:

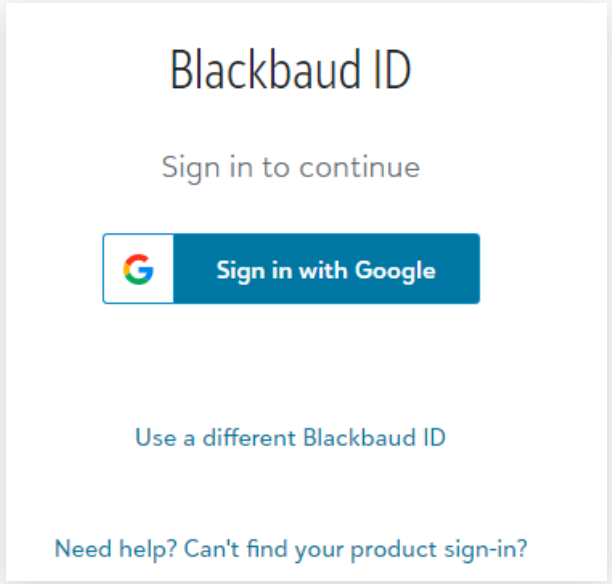
- **Email/Password**
- **SSO**
- **Social**

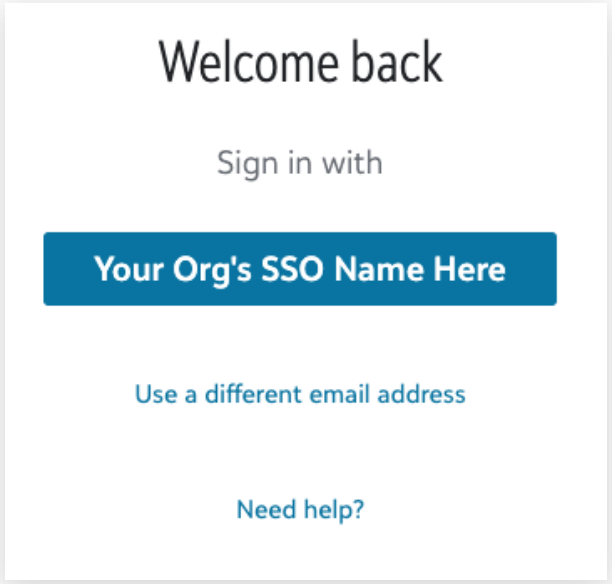
Use Case

- **Email/Password** users every time
- **SSO** users first time
- **Social** users first time
- Returning **Social** users
- Returning **SSO** users

Display



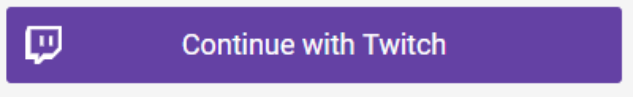


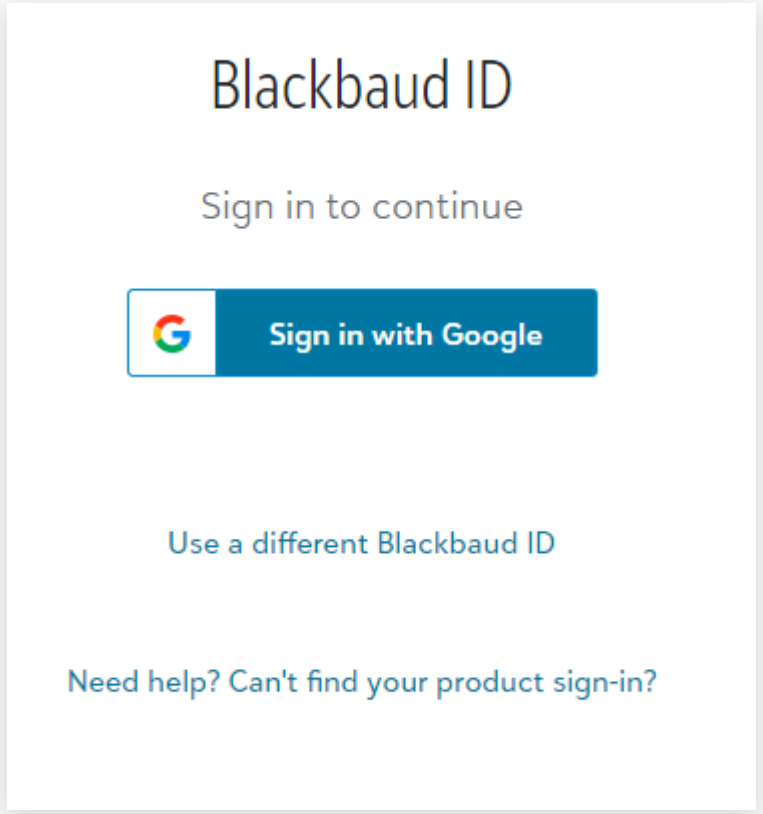


Signing in with Social Sign Ins

- Social Sign Ins make it easy for your consumers to access your site without creating a new set of credentials they must remember.
- No action is required of Admins for the use of Social Sign Ins.
- Today the only Social Sign In available on Blackbaud ID is Sign in with Google.
- When a user creates a Blackbaud ID, they can authenticate through Google. When users sign in with Google, they use Google for authentication requirements, password resets, and other support needs.

Other Social Sign Ins we're considering in the future include:





#bbdevdays

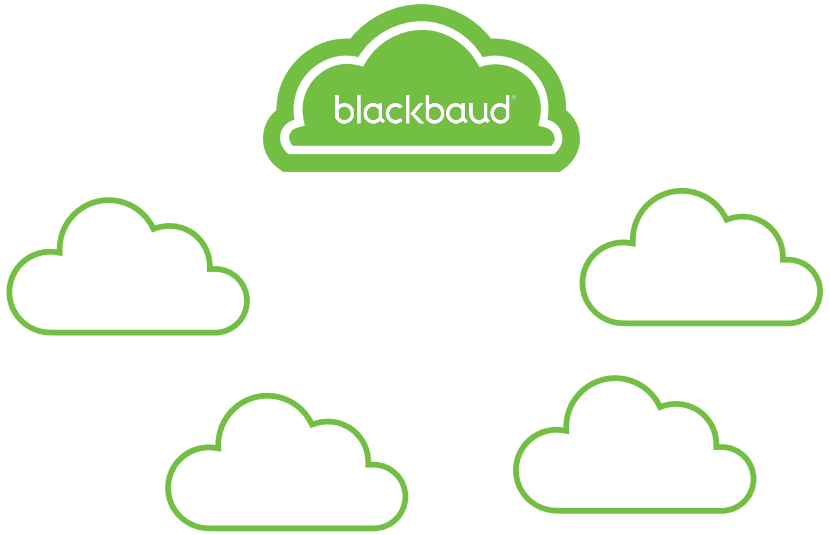
How should my Org manage authentication of our users with Blackbaud ID?

Consider your Org's Authentication Landscape

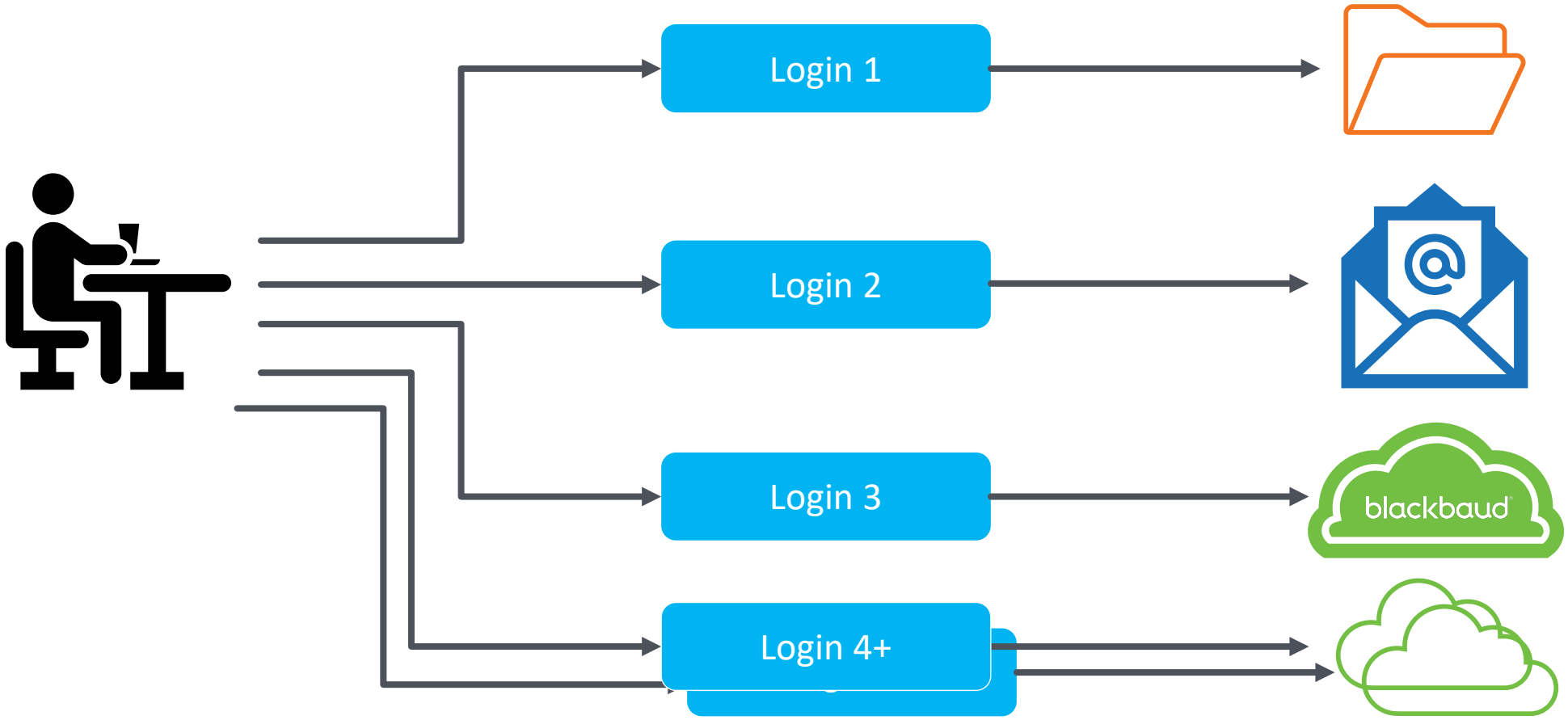
File sharing

Email

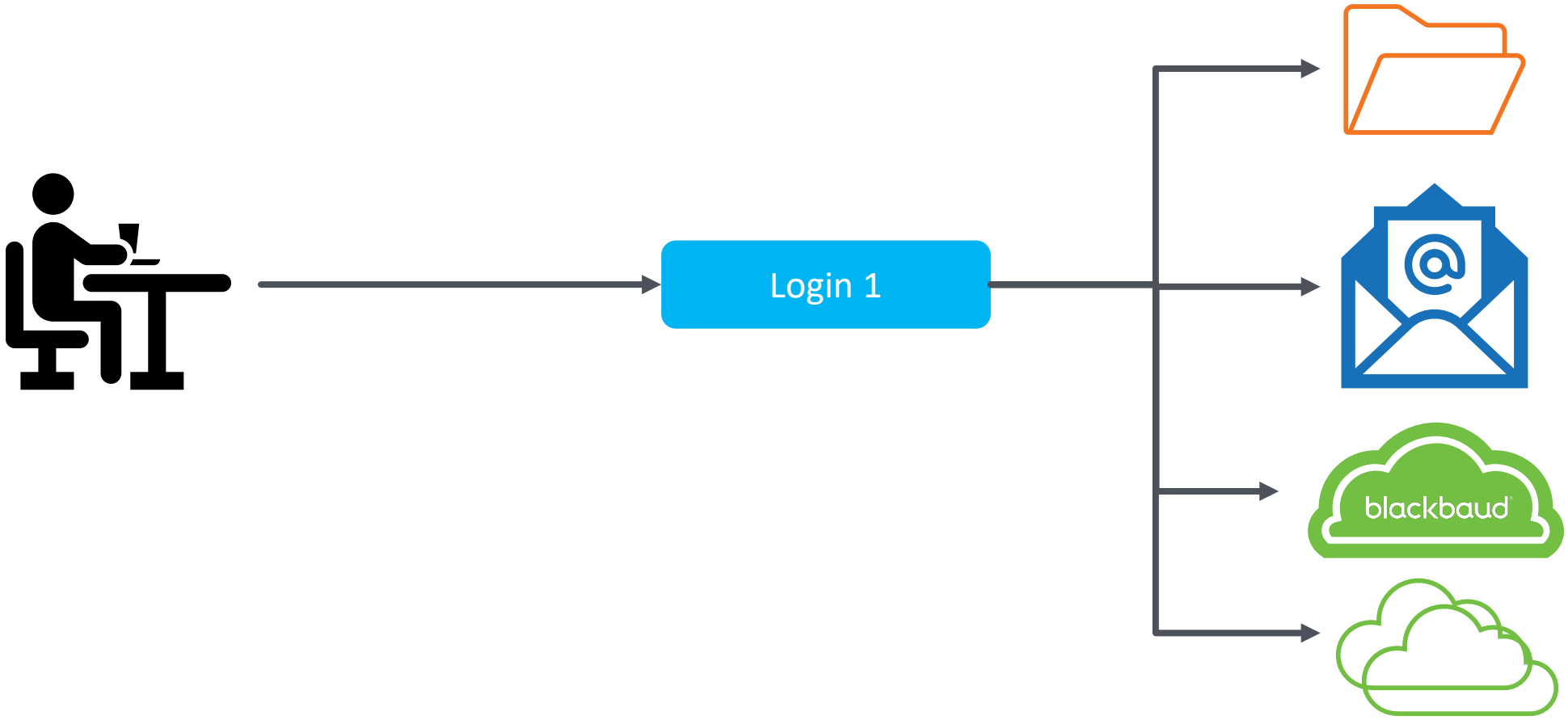
Other Business Applications



Without SSO



With SSO

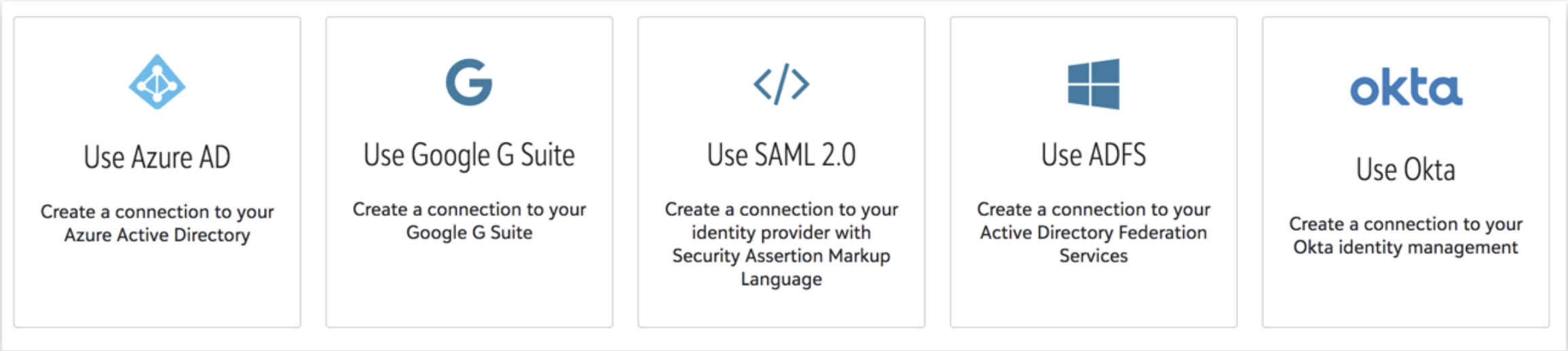


Should my org establish an SSO connection with Blackbaud ID?

- Does your org have an IdP with existing SSO connections? Then…
- Do you currently sign in to other cloud applications aside from Blackbaud? Then…
- Do you want to strengthen your org's security posture? Then…

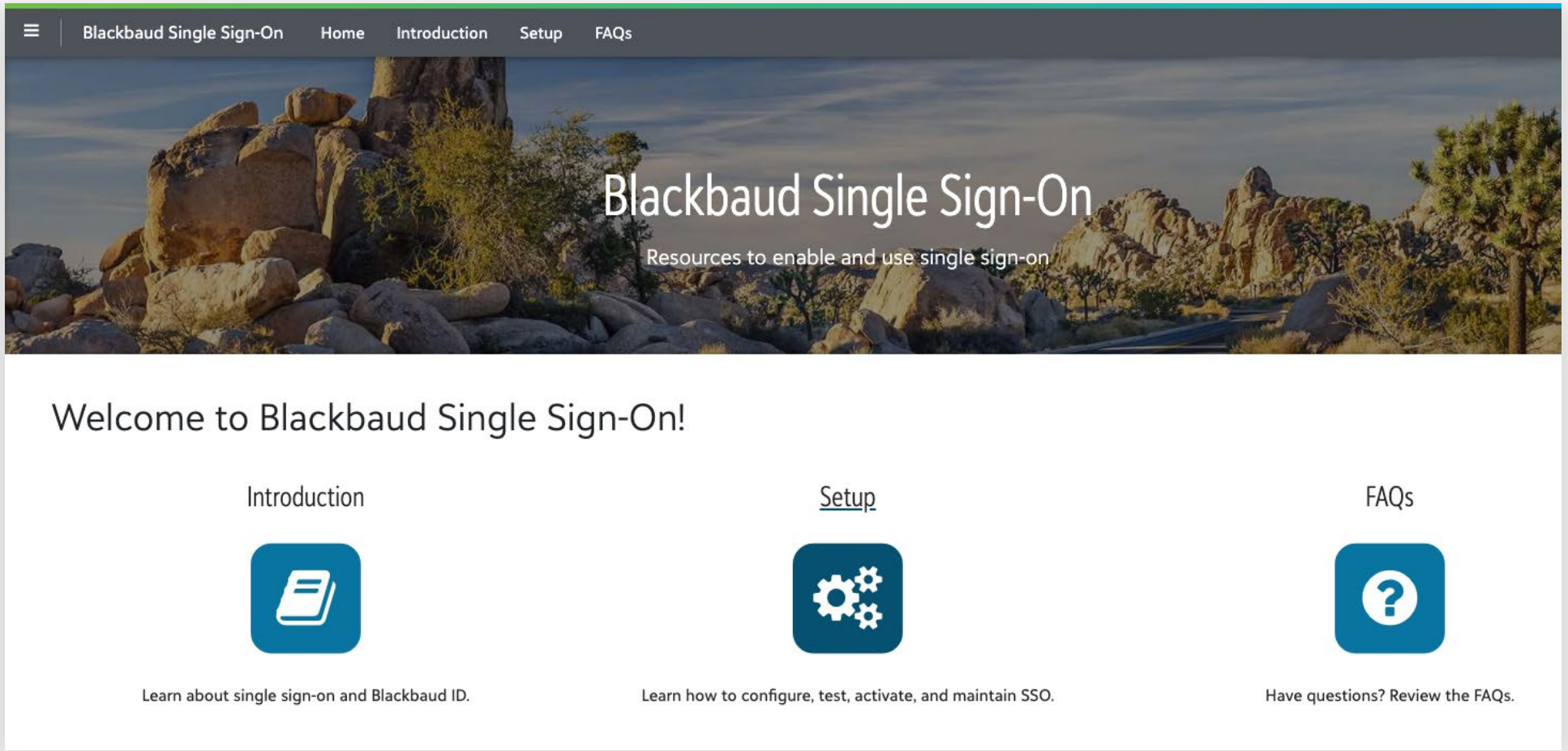
Signing in with SSO through IdP

If your org has an Identity Provider (IdP), then your Org Admin can create a SSO connection to Blackbaud ID using the options seen below so your colleagues have a single account across applications beyond Blackbaud.



For more background on Org Admins please see the replay of Demystifying Blackbaud SKY®.

Blackbaud ID Single Sign-On Resource Site

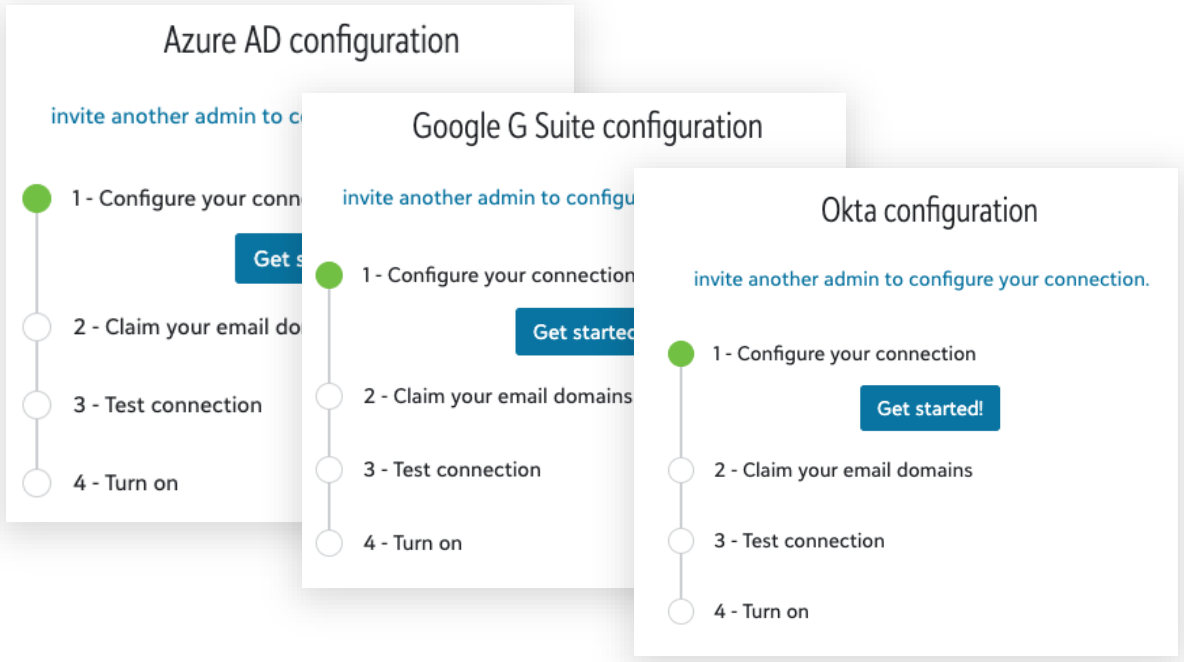


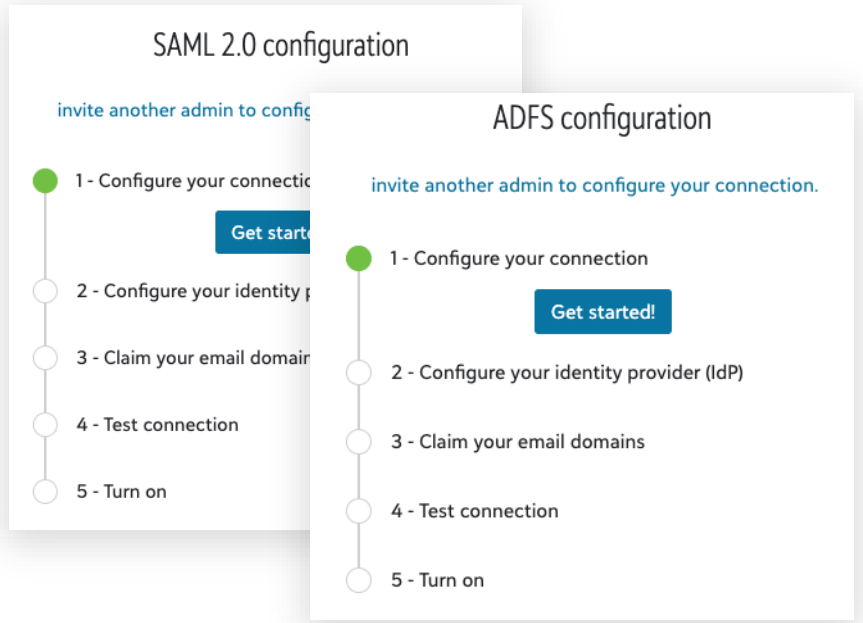
https://docs.blackbaud.com/sso-overview-docs/

What's involved with establishing an SSO connection with Blackbaud ID?

- There's 4-5 sections of the process depending on your IdP
- Takes less than 10 minutes if you're familiar with your IdP

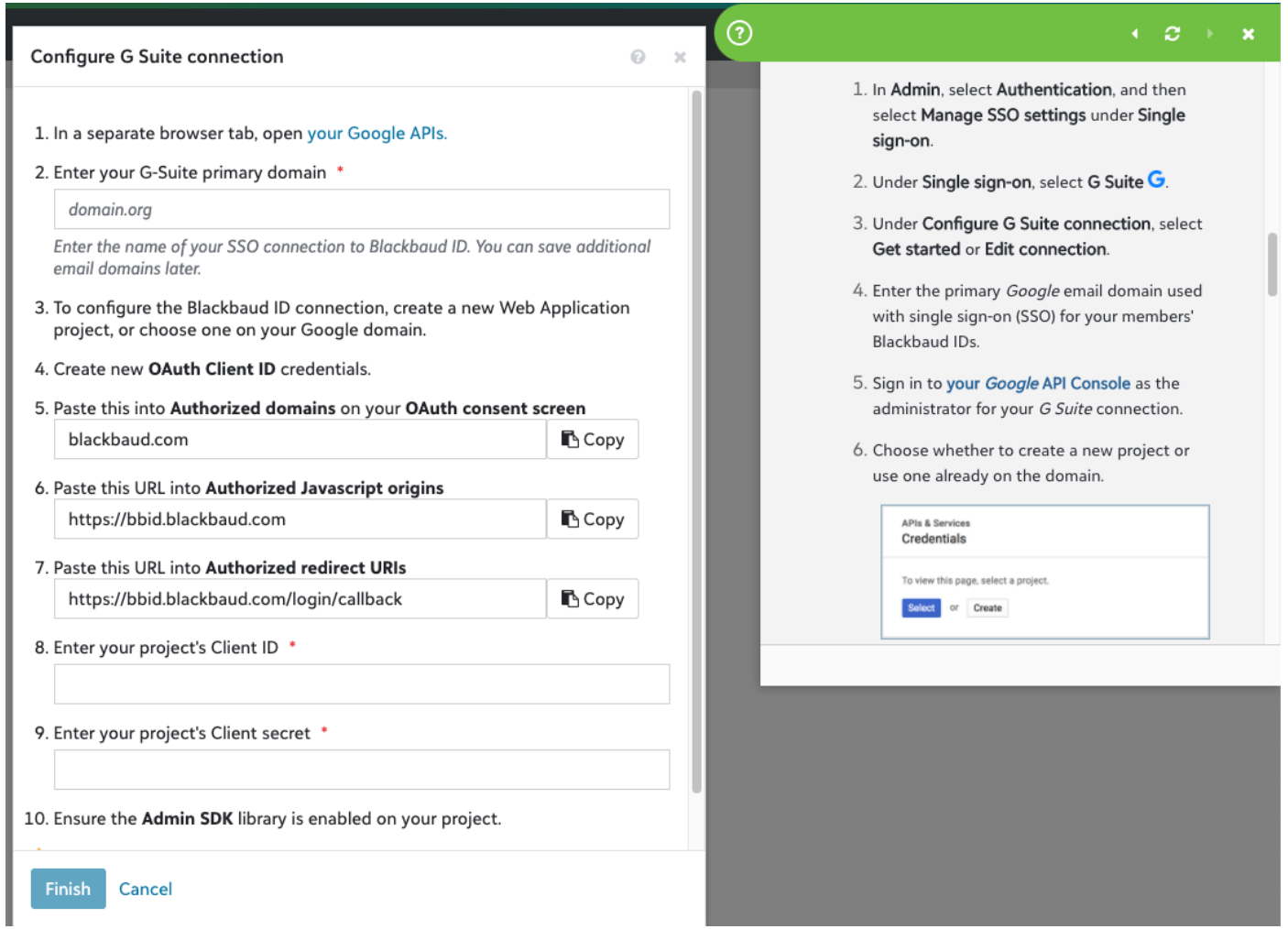
Tools you'll need for this job:
- Access to your IdP
- Ability to verify your DNS





SSO Setup Step by Step Instructions

Our instructions guide you through the setup process step by step for all SSO Connections.



#bbdevdays

Why care about MFA?

Less than 0.1%

Use of *anything* beyond the password significantly increases the costs for attackers, which is why **the rate of compromise of accounts using any type of MFA is less than 0.1% of the general population.**

Source: All your creds are belong to us!, Microsoft Blog

Blackbaud ID and MFA

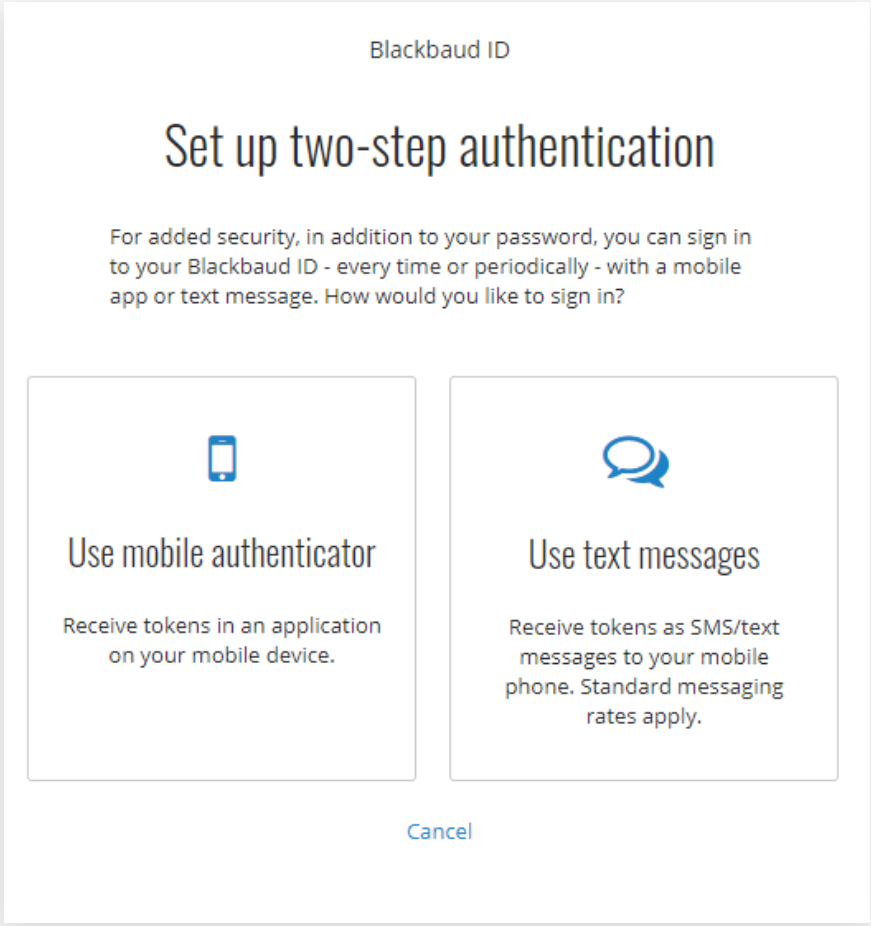
Having Multi-factor Authentication (MFA) turned on is the greatest single measure to increase the security of an account.

Enabling MFA on a Blackbaud ID account requires verification beyond email address and password. The verification can be achieved:

- Through a mobile authenticator with biometrics turned on such as fingerprint or facial recognition or time-based, one-time password (TOTP) application such as Google Authenticator, Microsoft Authenticator or Auth0 Guardian
- As SMS/text messages on mobile phone

Two items to keep in mind:

- To enforce MFA, Admins must establish a SSO connection using an IdP that allows enforcement of MFA.
- Users that have MFA turned on through their IdP do not need to turn it on within their Blackbaud ID account too as this creates 2 sets of verification codes to be entered



Who at your org should have MFA turned on?

- Application Admins
- Engineers
- Managers
- Sales
- HR
- Support
- And anyone else accessing sensitive, proprietary or confidential information on behalf of your org. Or to say…

Just about everyone

Are there groups to consider before requiring everyone to turn on MFA?

Yes

Considerations	Example
Access to a device for MFA	Children in school
What the user will be accessing	Congregant signing up for bible study
How long they'll be around	Volunteer helping people check in at an event

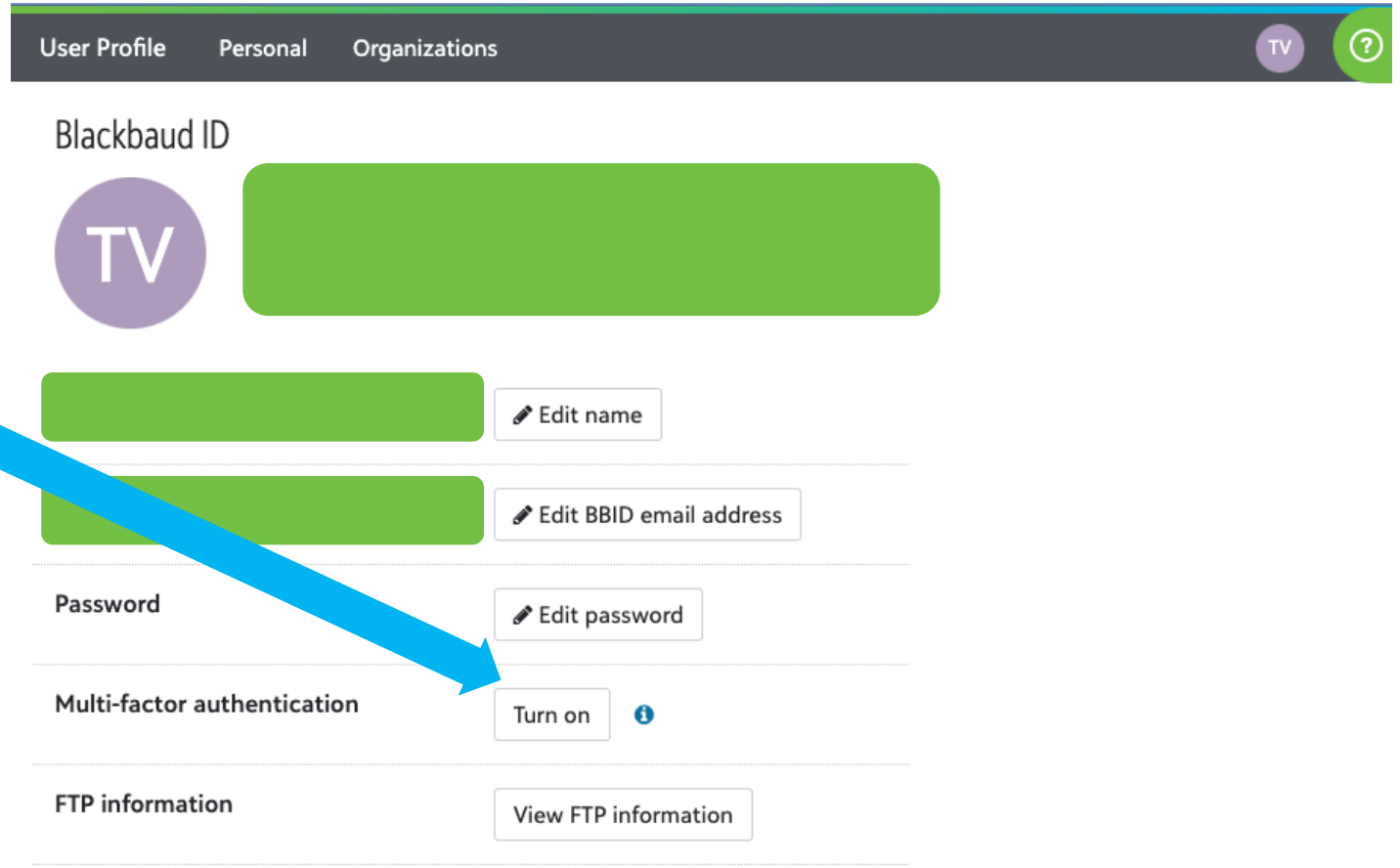
All this said, I don’t see my organization establishing an SSO connection with Blackbaud ID.

What should we do?

#bbdevdays

Turn on MFA available through Blackbaud ID

1. First visit your User Profile
2. Turn on MFA
3. Let your colleagues know how easy it is and advocate for them to use it.



Turning on MFA Step by Step – Mobile Authenticator

1. If necessary, download and install a mobile authenticator on your personal device. For more information, see **Mobile Authenticators**.
2. On **your Blackbaud ID profile**, select **Turn on** for **Multi-factor authentication**.
3. Enter your password, and select **Continue**.
4. Select **Use mobile authenticator** and **Next**.
5. To confirm your Blackbaud ID, scan the quick response (QR) code or enter the 16-character code in your mobile authenticator.
6. *Within five minutes*:
    a. Enter the verification code you receive on your device.
    b. To not require a verification code on the same device and browser for 30 days, select **Remember this browser**.
    c. Select **Next**.
7. Save the recovery code to use if you lose your mobile device, and select **Done**

Turning on MFA Step by Step - SMS

1. On **your Blackbaud ID profile**, select **Turn on** for **Multi-factor authentication**.
2. Enter your password, and select **Continue**.
3. Select **Use text messages**.
4. Enter the phone number to receive verification codes when you sign in, and select **Next**.
5. *Within five minutes*:
    a. Enter the verification code you receive on your device.
    b. To not require a verification code on the same device and browser for 30 days, select **Remember this browser**.
    c. Select **Next**.
6. Save the recovery code to use if you lose your mobile device, and select **Done**.

If you only remember 1 thing

The best way to strengthen your org's security posture is to have users authenticate with MFA through an IdP with established SSO connections to the applications used by your org.

#bbdevdays

Thank you!